Synopsis

Ph.D in Computer Science

Securing the VANET through a hybrid approach by Mitigating DoS Attacks and its types with Self-healing and Immunization

By

Ms. S. Rama Mercy

(17PHCSP011)

Supervisor

Dr. G. Padmavathi,

Department of Computer Science

Submitted to

Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore – 641 043

August 2024

Securing the VANET through a hybrid approach by Mitigating DoS Attacks and its types with Self-healing and Immunization

1. Introduction

Intelligent Transport System (ITS) refers to the integration of information and communication technologies into the transportation infrastructure to improve efficiency, safety, and sustainability. Vehicular Ad-hoc Network (VANET) is one of the core components of ITS being the indispensible reality of smart cities. The basic principle of VANET like Mobile Ad-hoc Network (MANET) is a self-organizing communication system that is not dependent on any infrastructure.

The architecture and the characteristics of VANET have the challenges such as Quality of Service (QoS), dynamic topology, connectivity, privacy and security still to be addressed. Security in VANET communication technology research and development efforts is crucial for maximizing the potential of intelligent transport systems [1][2] for secured message delivery enhancing traffic flow, relieving traffic congestion, and improving road safety. The security demanded by VANET is based on the integrity of data, confidentiality and availability.

Based on the security requirements, availability [3] is considered a significant factor in VANETs security guaranteeing that the network is functional and useful information is available at any functioning time. This critical security requirement for VANETs to ensure the users' lives remains as an important target for most of the attackers. Several attacks are in this category, the most prominent being the Denial of Service (DoS) attacks and its types. The DoS attack types extend to the Distributed Denial of Service (DDoS) attacks posing an even greater threat to VANETs due to their critical role in ensuring road safety. The severity and the consequences of the categories of DoS attacks and its types are highlighted in the below Figure 1. From the research work [4], there were twelve variants of DDoS attacks that pose significant security risks to VANETs and can disrupt vehicle communication, leading to potential safety hazards on the road.

2. Literature Study

The existing DoS/DDoS mitigation solutions for VANETs provide valuable insights for researchers and network administrators. By understanding their strengths, limitations, and trade-offs, more effective defenses to safeguard VANETs from these ever-evolving threats can be developed.

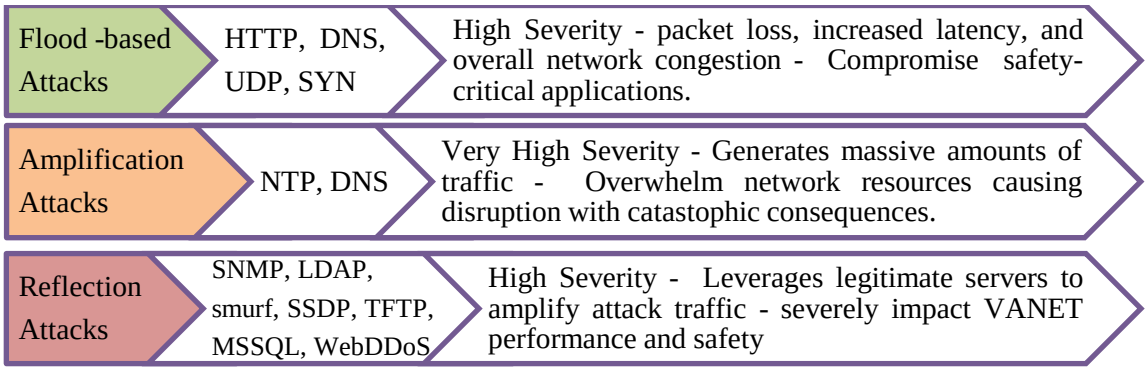
Flood -based Attacks
HTTP, DNS, UDP, SYN
High Severity - packet loss, increased latency, and overall network congestion - Compromise safety-critical applications.
Amplification Attacks
NTP, DNS
Very High Severity - Generates massive amounts of traffic - Overwhelm network resources causing disruption with catastophic consequences.
Reflection Attacks
SNMP, LDAP, smurf, SSDP, TFTP, MSSQL, WebDDoS
High Severity - Leverages legitimate servers to amplify attack traffic - severely impact VANET performance and safety

Figure 1: Severity of DoS Attacks and its types

The significance of the existing solutions to secure VANETs against DoS and DDoS attacks are elaborated in the Table 1 below.

Table 1: Review of VANET Security Solutions

Author, Year and Journal	Techniques/ Methods	Significance	Limitations
Tuka Kareem Jebur. (2023). Proposed Hybrid Secured Method to Protect Against DDOS in n Vehicular Adhoc Network (VANET). International Journal of Interactive Mobile Technologies (iJIM), 17(11), pp. 141–154. https://doi.org/10.3991/ijim.v17i11.38907.	Hybrid PSO-BAT Optimization Algorithm (HBPSO) Algorithm based on modified chaos - cellular neural network (Chaos - CNN) approaches proposed. Three-part - hybrid optimization search algorithm enhancing the route from source to destination, chaos theory detecting the abnormal nodes, then on Modified Chaotic CNN (MCCN) preventing malicious node from sending data. CICIDS dataset is used.	The Chaos - CNN approached results to outperform similar models of the related work and the approach protects the VANETs with high accuracy of 0.8736, specificity of 0.9959, TPR of 0.9561, and FPR of 0.78, Detection rate 0.9561.	The delete update and refresh operations, and storage is performed in the database at adjustable times. Reduce time prevent an attack and find the optimal path with reduced packet drop, average time will reduce.
R. Gopi, Mahantesh Mathapati, B. Prasad, Sultan Ahmad, Fahd N. Al-Wesabi, Manal Abdullah Alohali and Anwer Mustafa Hilal. (2022). Intelligent DoS Attack Detection with Congestion Control Technique for VANETs, Computers, Materials &	Two-stage processes namely, Teaching and Learning Based Optimization (TLBO) - based Congestion Control (TLBO-CC) and Gated Recurrent Unit (GRU)-based DoS detection (GRU-DoSD).	Reduced the level of congestion and detected the attacks. Optimization of the routes taken by vehicles. Effectively discriminated the compromised	The hyper parameter tuning of the GRU model can be derived by multi-objective TLBO algorithm in order to improve detection accuracy.

Continua. DOI: 10.32604/cmc.2022.023306.		and genuine vehicles and identified the DoS attacks.	
Bayat, M., Pournaghi, M., Rahimi, M. and Barmshoory, M. (2020). NERA: A new and efficient RSU based authentication scheme for VANETs. Wireless networks, 26, pp.3083-3098. https://doi.org/10.1007/s11276-019 -02039-x.	Road side unit (RSU) based scheme - the master key of the Trusted Authority (TA) is embedded in a tamper-proof device provided at the RSUs.	Performance and efficiency obtained.	Delay increases when the percent of vehicle equipped with OBU grows.
Mohammad Najafimehr., Sajjad Zarifzadeh., Seyedakbar Mostafavi., (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Engineering Reports. 2023;5:e12697. Wiley .	A comprehensive taxonomy of machine learning-based methods for detecting DDoS attacks, reviewing supervised, unsupervised, hybrid approaches, and analyzing the related challenges.	Various machine learning techniques have shown promise in detecting them.	Suggested development of robust defense mechanisms against DDoS attacks
Jim, L.E., Islam, N. and Gregory, M.A., 2022. Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. Computers & Security, 113, p.102538.	Artificial Immune System Based Algorithm (AISBA) without learning stage - principles of Artificial Immune Systems (AIS). Two different Trust models developed distinguishing a genuine node and a selfish node.	Average detection rate achieved - 93.41%. Compared with Secured AODV (SAODV) protocol with 87% (only 37% in SAODV) of PDR, 94% (only 86% in SAODV) detection rate.	Only detection focused.
N. Nishanth., A Mujeeb, (2021). Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Systems Journal, vol. 15, no. 1, pp. 17-26.	Mathematical modeling for SYN traffic in the network using Bayesian inference efficient algorithm.	The detection of SYN flooding attack using Bayesian inference defends any flooding-based DoS attack in a wireless ad hoc network with lower communication	Developed algorithm can be extended to different possible ways to detect various forms of DoS attack such as Hello flooding attack, SYN flooding attack, Black Hole attack, Jelly

		and memory overhead	Fish attack.
Aldhaheri et al., (2020). Deepdca: novel network-based detection of iot attacks using artificial immune system. Applied Sciences, 10(6), p.1909.	The hybrid framework used the Self Normalizing Neural Network and the Dendritic Cell Algorithm (DCA) (SNNN).	Streamlined and automated the signal extraction process, classification performance be improved.	This method needed too many detectors, and the system uses a negative selection technique in the sensing layer.

The highlighted past research works address the security solutions based on cryptography, machine learning, trust and artificial immune system. From the analysis, it is obvious that the existing VANET security solutions can be enhanced in terms of cryptographic techniques, intrusion detection based on AIS and machine learning based techniques. However, these techniques are with certain limitations such as such as high communication overhead, lack of efficiency, vulnerability to certain hybrid form of attacks, and a single point of failure for certificate revocation. The hybrid approaches adopted for securing the VANET are mentioned with its significance. The hybrid approaches are attempted recently for VANET security based on optimization algorithm, machine learning and deep learning.

The problem still exists to develop effective and efficient countermeasures to protect VANETs from various DoS attacks while preserving their real-time performance, reliability, and safety. In this research, one such attempt is made using the hybrid approach combining multiple security mechanisms to create a robust defense against DoS attacks and its types.

3. Problem Definition:

To secure Vehicular Ad-Hoc Networks in Intelligent Transportation System by detecting and mitigating DoS attacks

4. Objectives and scope of research work

The **major objective** of the research work is

To secure Vehicular Ad-Hoc Networks (VANETs) of Intelligent Transportation System against DoS attacks and its types by detection and mitigation with Self-healing and Immunization through a hybrid approach.

The secondary objectives that aim to fulfill the major objective are:

i. To detect and classify DoS attacks with improved accuracy of detection and classification, recall, precision, minimum delay through optimizing the features.
ii. To detect, predict and isolate (Mitigate) DoS attack and types with increased accuracy of detection, recall, precision, minimum delay, improved packet delivery ratio.

iii. To enhance the security and reliability of VANET services with minimum packet loss, maximum throughput, minimum processing time and maximum packet delivery ratio.

Secondary objective (i) focuses on the detection and classification of DoS attacks. It aims to improve the accuracy, recall, precision, and speed of this process through feature optimization. Secondary objective (ii) expands on this by adding prediction and isolation (mitigation) of DoS attacks to the scope and it also assesses towards the metric packet delivery ratio.

The scope of the research will focus on DoS attacks and its types considering the characteristics, challenges and the security requirements of the VANET. The security of VANET through the hybrid approach with the design, implementation and evaluation is applied. Thus, leveraging the strengths of multiple approaches to create a more effective and comprehensive solution with enhanced detection, proactive defense, resilience, adaptability.

5. Research Methodology

A three-phase methodology adopting the hybrid approach is followed to fulfill the mentioned objectives and addressing the challenges in securing the VANET. The proposed methodology in securing the VANET by mitigating DoS and DDoS attacks through the hybrid approach is shown in Figure 2.

The proposed three-phase methodology follows the hybrid approach by combining the machine learning, cryptography, deep learning, optimization and routing algorithms for securing VANET by mitigating DoS attacks and its types with self-healing and immunization.

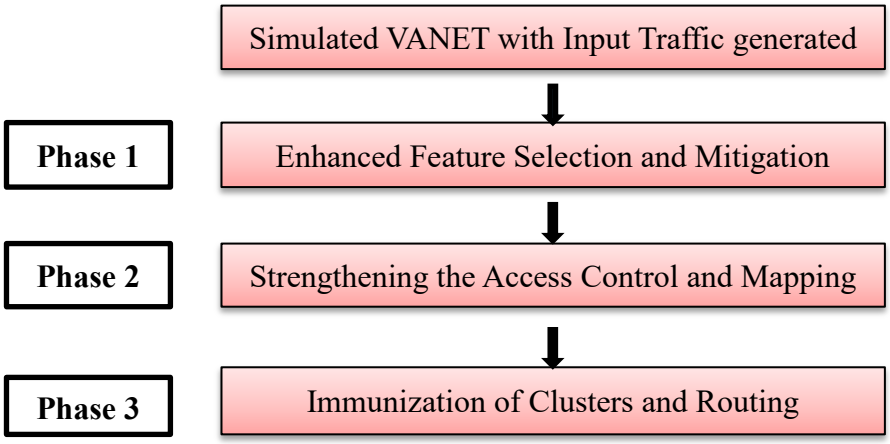
Simulated VANET with Input Traffic generated
Phase 1
Enhanced Feature Selection and Mitigation
Phase 2
Strengthening the Access Control and Mapping
Phase 3
Immunization of Clusters and Routing

Figure 2: Proposed Three-phase Methodology

The Phase 1 is to detect and classify the DoS and Botnet attacks using optimized feature selection and a classifier. The new DoS and DDoS attacks, the message rate, maximum limit and the elapsed time are considered for the feature selection. In addition,

the trustiness values with their relationships, the credibility score are considered for attack detection with classification and the self-healing effect mitigates the malicious vehicles from the VANET. The Phase 2 is to strengthen the traffic with trust nodes and encrypting the messages is implemented. In the process of strengthening the access control and mapping, the irrational nodes are detected and classified leading to routing efficiency. In Phase 3, improving the VANET security and resilience through immunization with proactive detection, isolation and routing is enforced.

The final phase evaluates the performance using various metrics, validating the results, and comparing them with the existing similar models. The results will demonstrate that the proposed hybrid approach performs well with immunized behavior of the clusters providing stability among changing topology and routing provided data transmission with reduced packet loss, delay and increased PDR.

6. Research Contributions

The overall research design as the hybrid approach with the contributions is depicted in the Figure 3.

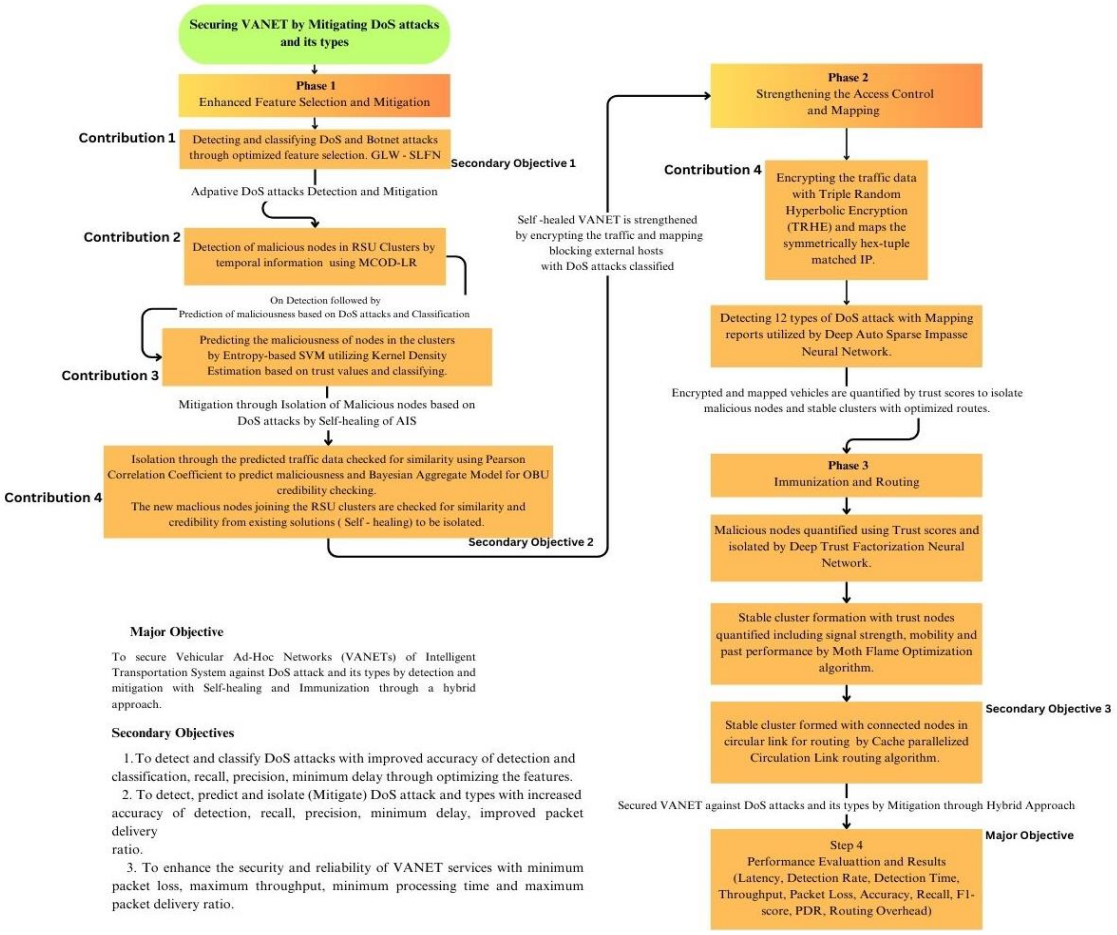
Securing VANET by Mitigating DoS attacks and its types
Phase 1
Enhanced Feature Selection and Mitigation
Contribution 1
Detecting and classifying DoS and Botnet attacks through optimized feature selection. GLW - SLFN
Secondary Objective 1
Adpative DoS attacks Detection and Mitigation
Contribution 2
Detection of malicious nodes in RSU Clusters by temporal information using MCOD-LR
On Detection followed by
Prediction of maliciousness based on DoS attacks and Classification
Contribution 3
Predicting the maliciousness of nodes in the clusters by Entropy-based SVM utilizing Kernel Density Estimation based on trust values and classifying.
Mitigation through Isolation of Malicious nodes based on DoS attacks by Self-healing of AIS
Contribution 4
Isolation through the predicted traffic data checked for similarity using Pearson Correlation Coefficient to predict maliciousness and Bayesian Aggregate Model for OBU credibility checking.
The new maclious nodes joining the RSU clusters are checked for similarity and credibility from existing solutions (Self - healing) to be isolated.
Secondary Objective 2
Self -healed VANET is strengthened by encrypting the traffic and mapping blocking external hosts with DoS attacks classified
Phase 2
Strengthening the Access Control and Mapping
Contribution 4
Encrypting the traffic data with Triple Random Hyperbolic Encryption (TRHE) and maps the symmetrically hex-tuple matched IP.
Detecting 12 types of DoS attack with Mapping reports utilized by Deep Auto Sparse Impasse Neural Network.
Encrypted and mapped vehicles are quantified by trust scores to isolate malicious nodes and stable clusters with optimized routes.
Phase 3
Immunization and Routing
Malicious nodes quantified using Trust scores and isolated by Deep Trust Factorization Neural Network.
Stable cluster formation with trust nodes quantified including signal strength, mobility and past performance by Moth Flame Optimization algorithm.
Stable cluster formed with connected nodes in circular link for routing by Cache parallelized Circulation Link routing algorithm.
Secondary Objective 3
Secured VANET against DoS attacks and its types by Mitigation through Hybrid Approach
Major Objective
Step 4
Performance Evaluattion and Results (Latency, Detection Rate, Detection Time, Throughput, Packet Loss, Accuracy, Recall, F1-score, PDR, Routing Overhead)
Major Objective
To secure Vehicular Ad-Hoc Networks (VANETs) of Intelligent Transportation System against DoS attack and its types by detection and mitigation with Self-healing and Immunization through a hybrid approach.
Secondary Objectives
1. To detect and classify DoS attacks with improved accuracy of detection and classification, recall, precision, minimum delay through optimizing the features.
2. To detect, predict and isolate (Mitigate) DoS attack and types with increased accuracy of detection, recall, precision, minimum delay, improved packet delivery ratio.
3. To enhance the security and reliability of VANET services with minimum packet loss, maximum throughput, minimum processing time and maximum packet delivery ratio.

Figure 3: Hybrid Approach with contributions in Securing VANET by Mitigating DoS attacks

The contributions fulfilling the major objective involve the objective function in maximizing the packet delivery ratio, minimizing the packet loss and maximizing the detection rate.

Phase 1 – Enhanced Feature Selection and Mitigation

The initial phase focus on the simulated VANET with generated traffic based on the CIC –IDS2018 and CIC-DDoS2019 datasets with attack information related to the VANET communications including new attacks in terms of reflection-based and exploitation-based attacks. In the phase 1 – Enhanced Feature Selection and Mitigation, the Glow-worm (GLW) swarm optimization technique with Single Layer Feed Forward Neural Network (SLFN) classifier is utilized to optimize the features relating to DoS attacks for detecting and classifying the DoS attacks and Botnet attacks. Further, the dynamic nature of the VANET required the adaptive attack detection and classification with self-healing effect of Artificial Immune System (AIS).

The flow of phase 1 is shown in Figure 4.

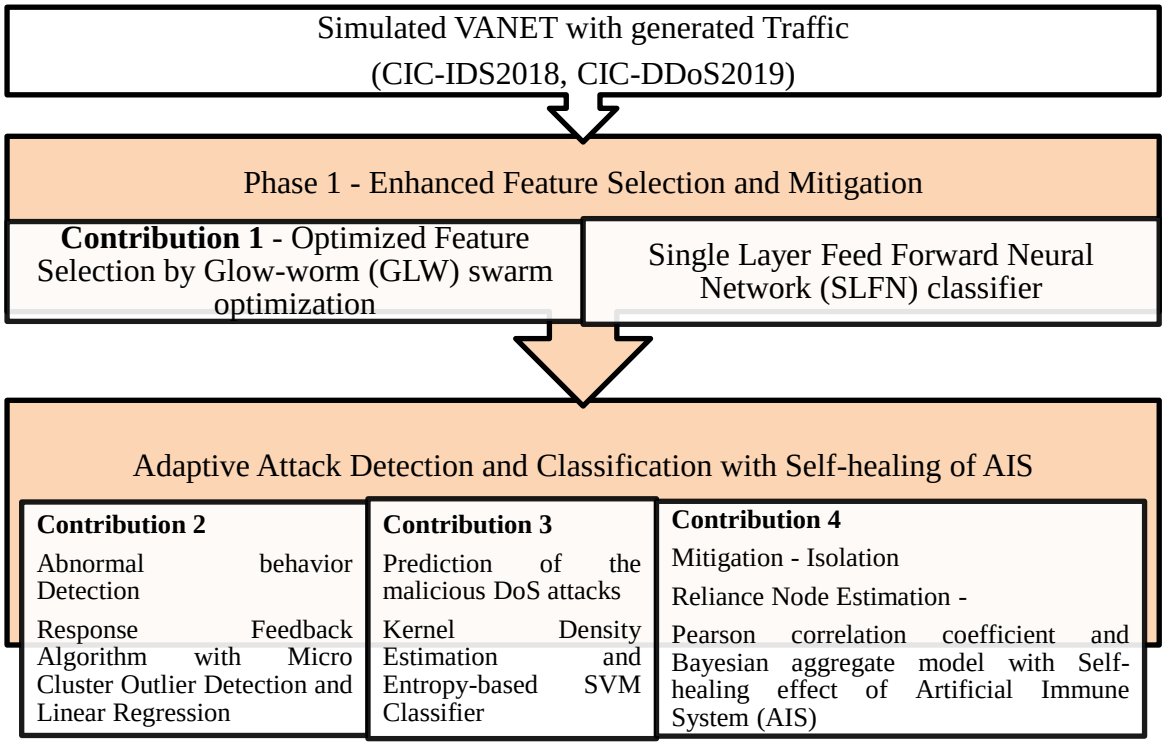
Simulated VANET with generated Traffic
(CIC-IDS2018, CIC-DDoS2019)
Phase 1 - Enhanced Feature Selection and Mitigation
Contribution 1 - Optimized Feature Selection by Glow-worm (GLW) swarm optimization
Single Layer Feed Forward Neural Network (SLFN) classifier
Adaptive Attack Detection and Classification with Self-healing of AIS
Contribution 2
Abnormal behavior Detection
Response Feedback Algorithm with Micro Cluster Outlier Detection and Linear Regression
Contribution 3
Prediction of the malicious DoS attacks
Kernel Density Estimation and Entropy-based SVM Classifier
Contribution 4
Mitigation - Isolation
Reliance Node Estimation -
Pearson correlation coefficient and Bayesian aggregate model with Self-healing effect of Artificial Immune System (AIS)

Figure 4: Flow of Phase 1-Enhanced Feature Selection and Mitigation

Contribution 1: Detection and Classification of DoS attacks using Glow-worm (GLW) Single Layer Feed Forward Neural Network (SLFN) Classifier

The proposed phase 1 is implemented with the optimized feature selection based on DoS and Botnet attacks using Glow-worm (GLW) swarm optimization. GLW fitness function is

formulated to detect the DoS attacks based on the optimum values obtained through the three stages. The global optimum value identifies features relevant to the local traffic and dynamically adjusted based on DoS and Botnet attacks. The SLFN classifier with the fitness function applied in selecting the optimized features through GLW detected DoS and Botnet attacks. The secondary objective 1 is fulfilled by the implementation of contribution 1 in detecting and classifying DoS attacks. The performance of contribution 1implementation is evaluated and compared based on the performance metrics based on learning kernel, time based on training and testing and accuracy.

The proposed contribution 1 exhibited improved accuracy in detection, sensitivity and selectivity than the existing machine learning algorithms. The results are shown in Figure 5.

S.No	Dataset details	Learning Kernel	Training Accuracy (%)	Testing Accuracy (%)
1	Five Feature Dataset	Sigmoid	95.5	95.4
		Sine	95.0	94.5
		Tanh	95.0	94.5

Types of Attacks	Time(secs)							
	Proposed GLW-SLFN		SLFN		RF		ANN	
	Training	Testing	Training	Testing	Training	Testing	Training	Testing
DoS attacks	0.233	0.109	0.345	0.108	0.298	0.118	4.56	2.39
BotNet attacks	0.231	0.112	0.3300	0.111	0.288	0.121	4.67	2.78

S.No	Algorithms	Performance Metrics	DoS Attacks (%)	Botnet Attacks (%)
1	Swarmfly-SLFN	Training Accuracy	87.5	86.45
		Testing Accuracy	87.0	86.0
		Sensitivity	86.0	84.0
		Specificity	85.0	83.0
2	BAT-SLFN	Training Accuracy	93	92
		Testing Accuracy	92.5	91.0
		Sensitivity	92	91
		Specificity	91.5	90.5
3	LDA-SLFN	Training Accuracy	94	94
		Testing Accuracy	93	93
		Sensitivity	90	90
		Specificity	90.5	90.5
4	Proposed GLW-SLFN	Training Accuracy	95.5	95.5
		Testing Accuracy	95.0	95.0
		Sensitivity	94.0	94.0
		Specificity	95.0	95.0

Figure 5: Performance of Contribution 1 and Comparison

Adaptive feature selection algorithms are to be implemented due to the dynamic nature of VANETs by continuously updating the selected feature subset as the network changes. Therefore, detection and mitigation of multiclass attacks of DoS are considered with the proposed contributions 2, 3 and 4 in the phase 1.

Contribution 2: Abnormal Behaviour Detection using Response Feedback Algorithm with Micro Cluster Outlier Detection Algorithm using Linear Regression (MCOD-LR)

The adaptive nature for the learning of maliciousness towards DoS attacks and then implementing the mitigation steps will secure the VANET. In this, the abnormal behaviour in the RSU clusters is first detected through the identification of features causing maliciousness. Features pertaining to malicious behavior are identified using Response Feedback Algorithm with MCOD-LR. The Response Feedback Algorithm considers the temporal information variable speed range based on data transmission and response time between the RSU, deviation from the packets sent and loss, the relative speed between vehicles and their position. MCOD-LR identifies the anomalous traffic indicative of DoS attacks due to the variation in data transmission, response time and change in network traffic, entropy values. The Mean Absolute Error (MAE) is derived based on the formula below and a lower MAE generally indicates better model performance in the DoS attacks based on accuracy and improving the latency.

As an ongoing process in securing VANETs, the abnormal behaviour in the RSU cluster detected must be continued with the changing topology along with prediction and classification of attacks based on DoS attacks. On detection of abnormal behaviour, DoS attacks are to be predicted and handled as the escalation of the maliciousness leading to the unavailability of the services.

The maliciousness of the attack caused by the network nodes are to be detected and classified and contribution 3 is proposed based on trust-based approach with the classifier for prediction and classification of DoS attacks.

Contribution 3: Prediction of Malicious DoS Attacks using Novel Adaptive Nodal Detection Algorithm with Kernel Density Estimation and Entropy-based Support Vector Machine (SVM) Classifier

Trust based approach implementing the kernel density estimation calculates the probability density function and generates the trustiness values for the parameters to assess the network for the maliciousness of the attacks. The parameters are vehicle density, average latency, packet delivery ratio, detection rate and energy consumption. The vehicle nodes affected in the RSU cluster network are identified by the calculated trustiness values exceeding the threshold values. The classifier Entropy-based SVM classifies the maliciousness type as it predicts the changes in the trust factor value and the kernel density estimation.

The abnormal behaviour in the RSU cluster detects and predicts with the classification as attack and no attack using Adaptive Nodal Attack Detection Algorithm. Attacks detected and predicted must be handled further to secure the network

. Contribution 4 is proposed to handle predicted attacks by isolation using reliance node estimation approach.

Contribution 4: Isolation using Reliance Node Estimation Approach using Pearson correlation coefficient and Bayesian aggregate model with Self-healing effect of Artificial Immune System (AIS)

The factors contributing to the vulnerability of DoS attack types are considered in addition to detecting the malicious behavior in the cluster network and the nodes. Securing the availability against such assaults is the main aim of this stage. The diverse functions in the quality of the RSU cluster network with variations in the similarity between the nodes, varied features and functionalities of various manufacturers of the vehicles are considered in this approach.

The trustiness identified in the clusters is then assessed for the similarities. The Pearson correlation coefficient can be used to measure the correlation between any two variables, including the vehicle density, energy consumption, packet delivery ratio (PDR), and detection rate of close nodes in a VANET. The quality of the RSU cluster communication with nodes availability and stability are focused due to the nodes density and the mobility using Pearson correlation method. In addition, onboard unit attached to the vehicle providing mobility with vehicular communication in appropriate direction is heterogeneous in nature based on the manufacturers.

The diverse features and functionalities of the vehicle nodes from the different manufacturers are vulnerable to assaults as OBUs continuously transmit information to other vehicles, roadside units (RSUs), and other devices in the form of Basic Safety Messages (BSMs). The credibility is checked using a Bayesian aggregate model based on the Pearson coefficient. The Bayesian aggregate model continuous to check the credibility of the RSU cluster communication network; therefore, if any vulnerability action is identified in the communication, the Bayesian aggregate model generates a credibility score of zero. The particular node is isolated with the self-healing effect of the Artificial Immune System (AIS). The self-healing effect of AIS with Pearson correlation coefficient is used to check the similarity of the predicted data with the VANET in the reliance node estimation approach in which the cluster network problems are resolved with the help of AIS.

The secondary objective 2 is fulfilled through contributions 2, 3 and 4 based on abnormal detection, prediction and classifying DoS attacks with mitigation. The performance of contributions 2, 3 and 4 are evaluated and the results are shown in Table 2.

Table 2 : Performance Evaluation of Contributions 2, 3 and 4

Network Size (No. of Nodes)	Number of Packets (p/sec)	Energy Consumption (EC) (J)	Latency (ms)	Detection Rate (%)	Throughput (Mbps)	Packet Loss (%)
50	9000	8	7	85	9.23	0.92
100	10000	15	10	86	10.23	0.9
150	11000	25	20	89	12.56	0.85
200	11000	38	30	97	15.03	0.78

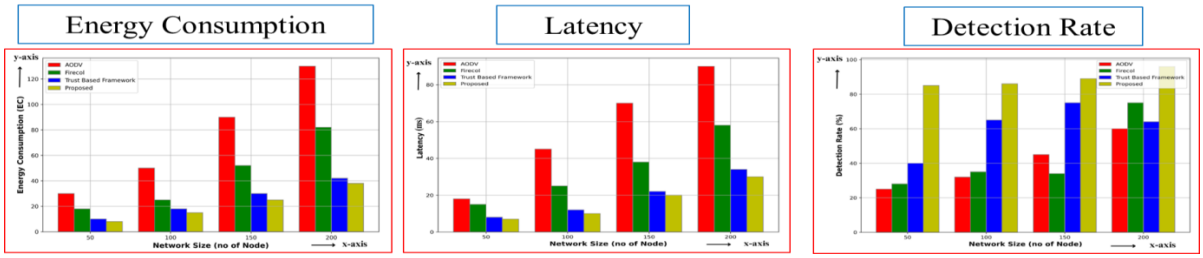

Figure 7: Performance Comparison of the Proposed Contributions 2, 3 and 4

Phase 1 with contributions 2, 3 and 4 provided Detection Rate of 97% with an increase of 1.2% in Detection Rate. DoS attacks detected and mitigated still needed attention on the links between vehicles that connect and disconnect very often making the communication and transmission difficult. VANET have to be secured from unauthorized access and new attacks in the changing topology. This necessitates securing the VANET to provide secured data transmission through optimized path reaching the destination vehicle bypassing the attacks. The flow of phase 2 and 3 is shown in Figure 8.

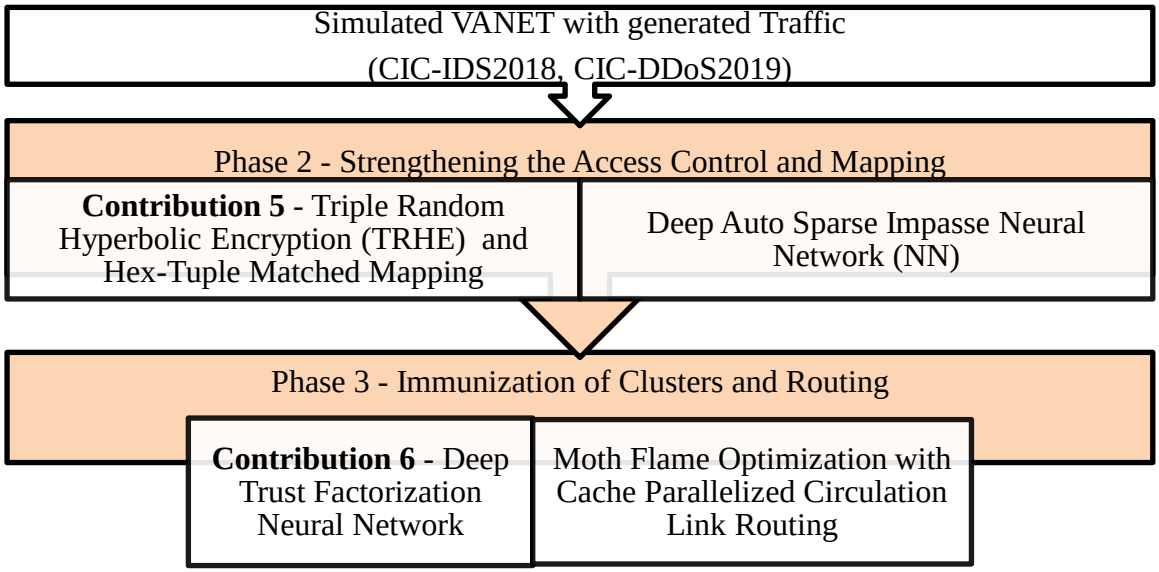
Simulated VANET with generated Traffic
(CIC-IDS2018, CIC-DDoS2019)
Phase 2 - Strengthening the Access Control and Mapping
Contribution 5 - Triple Random Hyperbolic Encryption (TRHE) and Hex-Tuple Matched Mapping
Deep Auto Sparse Impasse Neural Network (NN)
Phase 3 - Immunization of Clusters and Routing
Contribution 6 - Deep Trust Factorization Neural Network
Moth Flame Optimization with Cache Parallelized Circulation Link Routing

Figure 8: Flow of Phase 2 - Strengthening the Access Control and Mapping and Phase 3 – Immunization of Clusters and Routing

Phase 2 – Strengthening the Access Control and Mapping

The combined approach of the proposed contribution 5 with Triple Random Hyperbolic Encryption (TRHE) and Hex-Tuple Matched Mapping using Deep Auto Sparse Impasse Neural Network (NN) is applied to enhance the routing process by providing the secured traffic through mapped vehicles as rational with mapping report. The 12 variants of DDoS attacks are detected in this phase. The multi-class attack detection problem is addressed through the Deep auto sparse impasse NN. This is aided by Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping providing a report for routing in the next phase. AODV protocol in VANET is generally not considered as the best choice due to the broadcast storms and scalability limitations. In this phase, the routing process is eased for the protocol through the vehicles authorization thus providing secured data transmission.

Contribution 5: Strengthening the Access Control and Detecting DDoS Attacks using Triple Random Hyperbolic Encryption (TRHE) with Hex-Tuple Matched Mapping

The vehicles must also be authorized in receiving the data transmitted. Authentication of vehicle nodes and access privileges tend to be vulnerable due to various attacks. The TRHE is utilized to encrypt the data three times using a series of random hyperbolic transformations. The encrypted traffic received by the recipient is decrypted using the private key. This process would ensure that all the traffic signals in the VANET network are encrypted and protected from being intercepted or decrypted by unauthorized users. Encrypted traffic and vehicle mapping can be used together to improve the security by blocking external hosts and provide end-to-end network transparency.

Once the scanning is initiated, hex-tuple matched mapping is used to map all the same IP addresses in a symmetrically matching hex-tuple value. Over time, each node will develop a complete map of the network. N-1 mapping is a versatile and effective technique for mapping nodes in VANETs. It can be used to improve routing, safety. Deep Auto Sparse Impasse NN gathers the data from sensing and mapping reports to detect the attacker node on the network. Only a subset of connections or weights is active in the Deep Auto Sparse Impasse NN, with the remainder set to zero. Because zero-valued connections are not processed, the sparsity minimizes computing costs during training and inference. Consequently, fewer procedures are needed; resulting in quicker training time and this NN has high prediction accuracy for DDoS attacks. The mode used detects NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP DDoS attacks. The working of encryption and mapping with Deep Auto Sparse Impasse NN secured the VANET to provide safer routing and continued services further as proposed in contribution 6 of phase 3.

Phase 3 – Immunization of Clusters and Routing

The rapidly changing topology with the fluctuating changes in the network must consider interactions between the two vehicles and the history of the two vehicles for the continued services. To address the variations and provide continuous services without disruptions in network performance, contribution 6 is proposed with the deep neural network, Moth Flame Optimization (MFO) algorithm and Cache parallelized Circulation Link (CCL) routing. In this phase, identifying and isolating malicious vehicles with optimized best path detection and time and frequency synchronization base channel hopping on a network to effectively manage the dynamic fluctuation are achieved fulfilling the secondary objective 3.

Contribution 6: Immunization of clusters and routing through Deep Trust Factorization Neural Network with Trust Score and Moth Flame Optimization with Cache Parallelized Circulation Link Routing

The contribution towards enhancing the security and reliability is provided by the Deep Trust Factorization Neural Network (DT-NN) based on trust scores with identification and isolation of malicious vehicles. The reliability of VANET-based traffic information services and emergency response services are ensured based on the trust scores.

The stability is enforced for the transmission of data in vehicular networks through the optimization algorithms. Immunization, a technique inspired by biological immune systems, a promising approach enhances the resilience of VANETs against malicious attacks and enhance packet delivery ratio (PDR). The Moth Flame optimization (MFO) algorithm is a metaheuristic population-based algorithm inspired by the behavior of moths attracted to a flame effectively balance cluster formation and relation node selection in VANETs. This is applied in phase 3 with the objective to detect the best path in the network by updating each position in the node in enhancing the resilience of VANET.

The malicious nodes are reduced in the network by MFO-based immunization algorithm. Efficient routing of packets around congestion and malicious nodes is still a challenge with the random range of vehicle nodes. The Cache parallelized Circulation Link routing (CCL) is applied to make time and frequency synchronization base channel hopping on a network. This effectively manages the dynamic fluctuation of each node and removes the transmission of dangerous malware files on the network.

The working of contribution 6 started with cache routing introduced in which Deep trust factorization NN adds trust value for each node and the moth flame optimization is used to form a balance between the cluster to produce the high packet deliver ratio of 98% thereby detecting the malicious nodes and ensuring the linkage of each node in the cluster.

The performance of the phase 2 and 3 with contributions 5 and 6 in fulfilling the secondary objective 3 enhanced the security and reliability of VANET services by isolating the 12 variants of DDoS attacks during the dynamic fluctuation of VANET. VANET provided minimum packet loss, maximum throughput, minimum processing time and maximum packet delivery ratio as shown in Figure 9. The performance evaluated is compared with the existing approaches Trilateral Trust, H-IDS, Multi Filter and Stream Position Performance Analysis (SPPA) highlighting the outperformed hybrid approach as shown in Figure 10.

From the experimental results and based on the comparison made with the existing approaches, the proposed hybrid approach for securing the vehicular ad-hoc networks by mitigating denial of service attack and types with self-healing and immunization provided

- Transactions of the packet ratio secured and increased.
- Energy consumption reduced by isolating the malicious nodes.
- Detection rate increased to 97% based on the trustworthiness values of the vehicle nodes.
- Throughput considered higher reflecting the high transmission rate.
- The delay involved decreasing to 0.12 seconds and packet loss for each node decreasing by 0.5 bits.
- Detected the twelve variants DDoS attacks with an accuracy of 99% and less detection time of 0.1 ms

The phase 3 provided the immunity to the VANET network against the twelve types of hybrid DoS attack with the detection of the irrational nodes and forming a balance between the clusters to produce the high packet deliver ratio of 98% ensuring the linkage of each node in the cluster.

The research work developed a three-phase methodology to secure the vehicular ad-hoc networks by mitigating DoS attacks and its types through the hybrid approach fulfilled the major objective and the secondary objectives thus ensuring reliability of VANET services. The contributions achieved minimized packet loss of 0.5 bits and maximized attack detection rate of 97%.

The performance obtained based on the metrics are inferred through the contributions. Contribution – 5: Triple random hyperbolic encryption (TRHE) with hex tuple matched mapping and Deep Auto Sparse Impasse NN provided high accuracy by extracting features from sensing and mapping report to detect hybrid DDoS attacks.

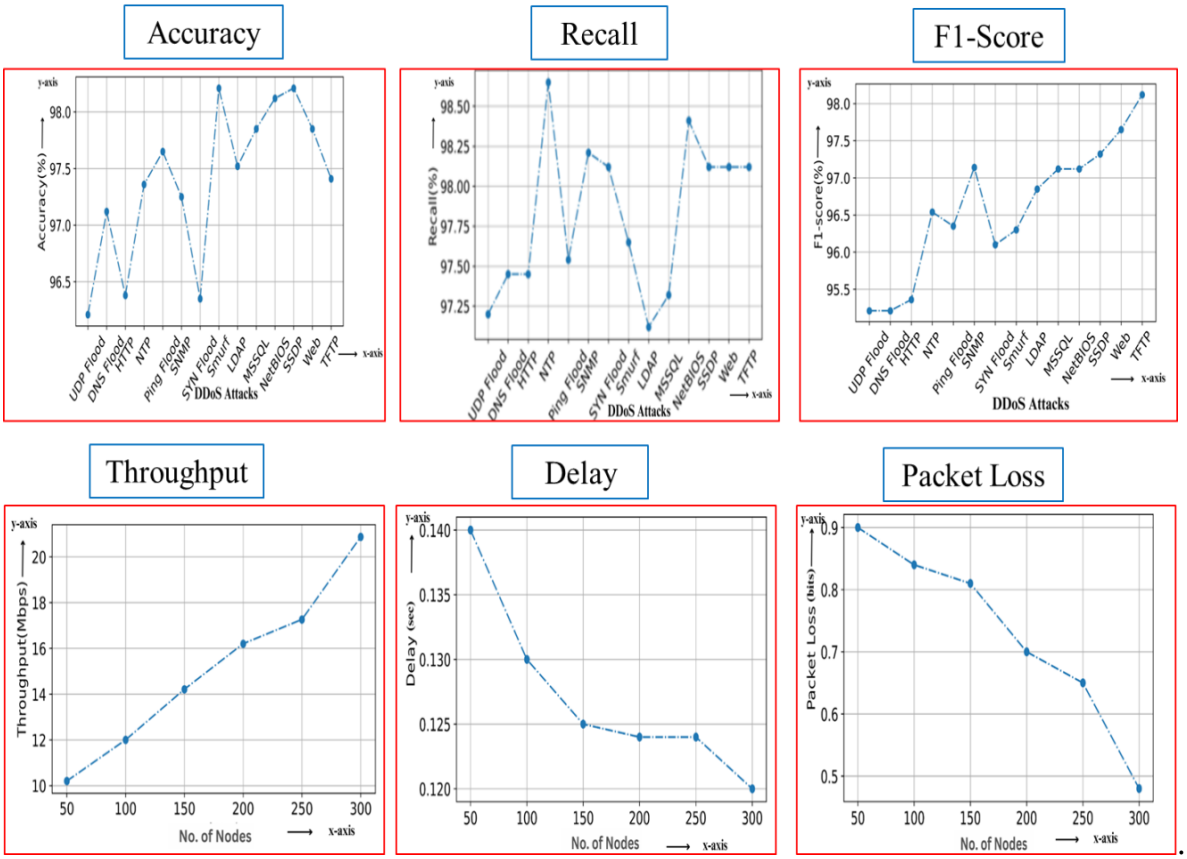

Figure 9: Performance of the Proposed Contributions 5 and 6 of Phase 2 and 3

Hex tuple matched mapping provided high recall by same IP address mapped using a hex-tuple value. Hex tuple matched mapping by same IP address mapped using a hex-tuple value and Deep Auto Sparse Impasse NN provided high F1- Score in detecting hybrid DDoS attacks.

Contribution – 6: Cache parallelized circular link state routing adopts time and frequency synchronization channel hopping to get a high delivery ratio, minimized packet delay and packet loss. The performance is assessed through the comparison and the contributions 5 and 6 outperformed the performance of the existing approaches based on the following inferences.

Contribution – 5: Triple random hyperbolic encryption (TRHE) with hex tuple matched mapping and Deep Auto Sparse Impasse NN provided high accuracy by extracting features from sensing and mapping report to detect hybrid DDoS attacks.

Cache parallelized circular link state routing adopts time and frequency synchronization channel hopping with hex tuple matched mapping contributes to low overhead high packet delivery ratio.

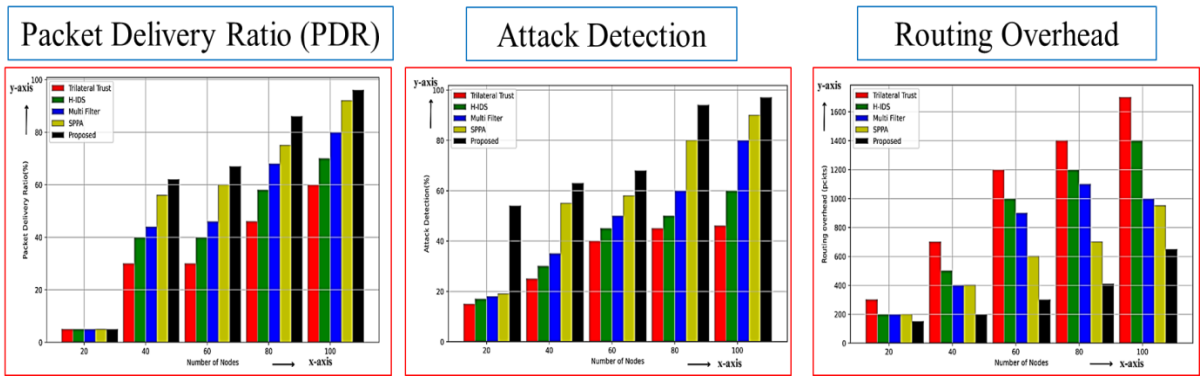

Figure 10: Performance Comparison of the Proposed Contributions 5 and 6

The parameters life and fall based on the objective function in securing VANET are considered on the following factors.

- Dynamic network conditions: Changes in traffic density, vehicle speed, and environmental factors can impact packet life and loss rates.
- Evolving attack patterns: New types of DoS attacks with different characteristics can affect the life and fall of detection and mitigation mechanisms.

The proposed hybrid approach in fulfilling the major objective focused on the attainment of the performance based on the optimization of cluster formation through MFO with the selection of reliable relay nodes with high Packet Delivery Ratio (PDR) and isolating malicious nodes. MFO is one such multi-objective optimization techniques utilized in fulfilling the major objective by considering the optimization of one attribute high PDR related to ensuring efficient data delivery.

The contributions are devised to secure the VANET based on the mentioned factors to sustain the reliability of the VANET services in minimizing the rate at which packets are dropped and maximizing the ability to detect the DoS attacks and mitigate.

7. Summary, Conclusion and Future Scope

The research work entitled “Securing the VANET through the Hybrid Approach by Mitigating DoS attacks and types with Self-Healing and Immunization” is a three-phase methodology using the hybrid approach with 6 significant contributions fulfilled the major and secondary objectives and addressed the challenges in securing the VANET. The proposed security approach pertaining to the self-organized network with communications among nearby vehicles and fixed road infrastructure have high dynamism, unbounded, scalable, heterogeneity challenges can be applied for the real-time applications. Real-time applications like supply chain management, where timely and accurate information is paramount can be aligned with VANET services.

Future research can be explored based on the following aspects:

Enhanced Performance: The proposed three-phase methodology enforced encryption technique for secured transmission. Developing strong privacy to further enhance VANET performance can be explored. Optimization techniques adopted for the immunization based on Moth-Flame Optimization relies on high PDR for efficient data delivery. Considered as a single attribute objective function focused towards stable clusters with reliable relay nodes can be explored based multi attribute optimization for scalability, optimize communication efficiency, reliability. There exists the scope for future enhancement based on enhanced performance of VANET with enhanced security against DoS attacks and its types through multi-objective optimization, privacy-preserving techniques.

8. Publications

Journals

- Rama Mercy Sam Sigamani and Padmavathi Ganapathi, GOF-SLFN- An Intelligent Attack Detection System against Denial of Service (DoS) attacks based on Glow Worm Swarm optimized Single Layer Feed Forward Networks for vehicular Cyber Physical Systems (VCPS), IOP Conference Series: Materials Science and Engineering, Volume 925, 13th October, 2020. https://iopscience.iop.org/article/10.1088/1757-899X/925/1/012001
- Rama Mercy. S., G. Padmavathi, Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANET, International Journal of Computer Network and Information Security(IJCNIS), Vol. 15, No. 3, Jun. 2023 - indexed in Scopus from 2020 to present with an impact factor of 1.5. https://www.mecs-press.org/ijcnis/v15n3.html.
- Rama Mercy. S., G. Padmavathi, Encrypted Access Mapping in a Distinctly Routed Optimized Immune System to Prevent DoS Attack Variants in VANET Architecture (IJCNIS), Vol. 16, No. 3, Jun. 2024 - indexed in Scopus from 2020 to present with an impact factor of 1.5. https://www.mecs-press.org/ijcnis/ijcnis-v16-n3/v16n3-8.html.

Conference

- Participated and presented paper Impact of Artificial Immune Systems in Securing Intelligent Transportation Systems, in 12th International Conference on Recent Challenges in Engineering and Technology (ICRCET-2024) Organized by Institute for Education Research and Publication (IFERP) held on 23rd-24th April 2024, Aloft Bengaluru Whitefield, Bangalore, India.

9. Significant References

[1] Sheikh, Muhammad Sameer, Jun Liang, and Wensong Wang. 2019. "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)" *Sensors* 19, no. 16: 3589. https://doi.org/10.3390/s19163589.

[2] Mishra, R., Singh, A. and Kumar, R., 2016, March. VANET security: Issues, challenges and solutions. In 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT) (pp. 1050-1055). IEEE.

[3] Muhammad Sameer Sheikh, Jun Liang. 2019. A Comprehensive Survey on VANET Security Services in Traffic Management System. Wireless Communications and Mobile Computing, Wiley Online Library. https://doi.org/10.1155/2019/2423915.

[4] Tuka Kareem Jebur. (2023). Proposed Hybrid Secured Method to Protect Against DDOS in n Vehicular Adhoc Network (VANET). International Journal of Interactive Mobile Technologies (iJIM), 17(11), pp. 141–154. https: // doi.org/ 10.3991/i jim.v17i11.38907.

[5] R. Gopi, Mahantesh Mathapati, B. Prasad, Sultan Ahmad, Fahd N. Al-Wesabi, Manal Abdullah Alohali and Anwer Mustafa Hilal. (2022). Intelligent DoS Attack Detection with Congestion Control Technique for VANETs, Computers, Materials & Continua. DOI: 10.32604/cmc.2022.023306.

[6] Bayat, M., Pournaghi, M., Rahimi, M. and Barmshoory, M. (2020). NERA: A new and efficient RSU based authentication scheme for VANETs. Wireless networks, 26, pp.3083-3098. https:// doi.org/10.1007/s11276-019 -02039-x.

[7] Mohammad Najafimehr., Sajjad Zarifzadeh., Seyedakbar Mostafavi., (2023). DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Engineering Reports. 2023;5:e12697. Wiley.

[8] Jim, L.E., Islam, N. and Gregory, M.A., 2022. Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. Computers & Security, 113, p.102538.

[9] N. Nishanth., A Mujeeb, (2021). Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Systems Journal, vol. 15, no. 1, pp. 17-26.

[10] Aldhaheri, S., Alghazzawi, D., Cheng, L., Alzahrani, B. and Al-Barakati, A., 2020. Deepdca: novel network-based detection of iot attacks using artificial immune system. Applied Sciences, 10(6), p.1909.60-969.

[11] Alrehan AM, Alhaidari FA. Machine learning techniques to detect DDoS attacks on VANET system: a survey. Paper presented at: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). 2019:1-6.

[12] Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M. and Ma, M., 2019. Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics. IEEE ccess, 7, pp.158481-158491.

[13] Kolandaisamy, R., Noor, R.M., Kolandaisamy, I., Ahmedy, I., Kiah, M.L.M., Tamil, M.E.M. and Nandy, T., 2021. A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. Journal of Ambient Intelligence and Humanized Computing, 12(6), pp.6599-6612.

[14] Ahmed, S., Rehman, M.U., Ishtiaq, A., Khan, S., Ali, A. and Begum, S., 2018. VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead. Journal of Sensors, 2018.

[15] Li, W. and Song, H., 2015. ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE transactions on intelligent transportation systems, 17(4), pp.9.